KASPERSKY LAB

Kaspersky Anti-Virus 5.5 for Lotus Notes/Domino

User's guide

USER'S GUIDEKASPERSKY ANTI-VIRUS 5.5
FOR LOTUS NOTES/DOMINO

User's Guide

© Kaspersky Lab
http://www.kaspersky.com
Revision date: March, 2006

Table of Contents

CHAPTER 1. KASPERSKY ANTI-VIRUS 5.5 FOR LOTUS NOTES/DOMINO 5
1.1. What's new in version 5.5? 6
1.2. Hardware and software system requirements 7
1.3. Distribution kit 8
1.3.1. License Agreement 8
1.3.2. Registration card 9
1.4. Services provided for registered users 9
1.5. Conventions 9

CHAPTER 2. INSTALLING THE APPLICATION 11
2.1. Installing the application 11
2.2. Performing post-installation setup 13
2.3. Removing the application 14

CHAPTER 3. KASPERSKY ANTI-VIRUS INTERNAL ARCHITECTURE 15

CHAPTER 4. CONFIGURING THE ANTI-VIRUS PROTECTION SYSTEM 17
4.1. General settings of Kaspersky Anti-Virus operation. Tasks configuration/General 17
4.2. Updates settings. Tasks configuration/Updates configuration 18
4.3. Replications scan settings. Tasks configuration/ Replications configuration 21
4.4. E-mail messages scan settings. Tasks configuration/E-mail scan 23
4.5. Anti-virus protection settings. Tasks configuration/Protection against virus outbreaks 25
4.6. Database scan settings. Tasks configuration/Database scan 26
4.7. Anti-virus protection settings. The *Anti-virus kernel* section 28
4.7.1. Anti-virus kernel/General 28
4.7.2. Anti-virus kernel/Actions 29
4.7.3. Notifications 31

CHAPTER 5. ADDITIONAL SETTINGS 33
5.1. Quarantine database 33
5.1.1. Working with documents in the quarantine database. Quarantine database/Databases 34

5.1.2. Working with e-mail message objects in the quarantine database. Quarantine/E-mail messages 36
5.2. Worklog 38
5.3. Anti-virus statistics 39
5.4. Working with license keys 41
5.4.1. Managing license keys 41
5.4.2. Renewing your license 42
5.5. Managing the application using command line 43

CHAPTER 6. VERIFYING THE APPLICATON'S OPERATION 45

APPENDIX A. FREQUENTLY ASKED QUESTIONS 47

APPENDIX B. KASPERSKY LAB 51
B.1. Other Kaspersky Lab Products 52
B.2. Contact Us 56

CHAPTER 1. KASPERSKY ANTI-VIRUS 5.5 FOR LOTUS NOTES/DOMINO

Kaspersky Anti-Virus™ 5.5 for Lotus Notes/Domino (hereinafter referred to as Kaspersky Anti-Virus, application) is designed to provide anti-virus protection of Lotus Notes/Domino-based mail systems. The application is installed on the server running Windows NT/2000/XP/2003 operating system and protects all mail traffic passing through the server and of the Domino database files against malware.

Kaspersky Anti-Virus for Lotus Notes/Domino performs the following functions:

- *scanning for viruses all e-mail messages passing through the Lotus Notes mail system installed on this server*. The anti-virus scan involves both the text of the message and attached files. Additionally, Kaspersky Anti-Virus scans for viruses inside attached archives and packed exe files, as well as inside attached mail format files and e-mail database files.

- *disinfection of virus-infected messages* if this is provided for by the settings. Kaspersky Anti-Virus can disinfect both the text of the message and attached files.

- *filtering database files by the name and by the extension* as defined by the settings. Files of this type will be treated using processing specific rules defined by the administrator.

- *saving infected objects* in a special quarantine storage that rules out the possibility of data loss.

- *notifying* the sender, recipient and the system administrator about messages that contain malicious objects.

- *registering virus outbreaks and notify about such events*. The application registers attempts of mass mailing of infected messages.

- *updating anti-virus database* either in automatic or manual mode. Update resources include Kaspersky Lab's ftp and http servers or a local/network folder that contains an up-to-date set of updates.

- maintaining the operation log and statistical database about the operation of the application.

- managing license keys.

The application can be configured by any administrator who has an access to the configuration database (see section 4.1, page 16).The application can be configured from a workstation on which the Lotus Notes client application is installed.

Attention! New viruses every day and in order to keep your anti-virus application up-to-date, it is extremely important that you update your *anti-virus database* on an hourly basis!

Please note limitations in the operation of Kaspersky Anti-Virus for Lotus Notes/Domino:

- it does not scan messages encrypted using a sender's privacy key;
- it destroys the integrity of the electronic signature for messages signed by the sender when adding a scan report to the text of the message or when replacing attached files with disinfected files;
- it dos not scan files created in OS/2 or Macintosh environment;
- it converts messages from MIME format into Rich Text if a scan report is added to the body of the message. Some formatting feature of the message may be lost.
- it cannot be configured through the web interface.

1.1. What's new in version 5.5?

Version 5.5 of Kaspersky Anti-Virus for Lotus Notes/Domino has been considerably enhanced compared to version 5.0, namely:

- The application architecture has been modified to exclude storing e-mail messages in an intermediate mailbox before performing the anti-virus scan and mail flow processing. Now this step is not required and the scan process has been drastically streamlined.
- The Kavupdater component, that performs the anti-virus database the application anti-virus kernel updates, has been modified.
- An ability to perform an anti-virus scan and processing of replications performed by the Domino server.
- The server installation of the application has been made analogous to the installation process performed on a computer running Windows OS.

1.2. Hardware and software system requirements

The following software shall be installed on the server for the operation of Kaspersky Anti-Virus for Lotus Notes/Domino:

One of the following operating systems:

- Windows 2000 (Service Pack 4 and higher)
- Window 2000 Advanced Server (Service Pack 4 and higher)
- Windows Server 2003 Standard Edition
- Windows Server 2003 Enterprise Edition

One of the following versions of Lotus Notes/Domino:

- version 5.0.10 and higher;
- version 6.5 and higher.
- version 7.0 and higher.

Lotus Notes/Domino 7.0 version is supported without the use of the DB2 Universal Database technology.

General system requirements:

- Pentium 300 MHz or higher processor;
- 64 MB free RAM (128 MB is recommended).
- 11 MB of free disk space in order to install the application (without taking into account the space required for the backup storage and other service folders).

The free disk space required is calculated based on the average size of one message.

The system requirements for Lotus Domino may differ from the system requirements for Kaspersky Anti-Virus. Make sure that your system configuration complies with the system requirements for both products!

1.3. Distribution kit

You can purchase Kaspersky Anti-Virus either from our dealers (retail box) or online (for example, visit http://www.kaspersky.com and follow the **E-Store** link).

The retail box package includes:

- a sealed envelope with the installation CD containing the application files;
- User's Guide
- a license key written on the installation CD or on a special diskette;
- registration card (containing the serial number of the product);
- License Agreement

Before you open the envelope with the CD make sure that you have carefully read the license agreement...

If you buy Kaspersky Anti-Virus online, you will have to download the application from the Kaspersky Lab's website. In this case, the distribution kit will include this Guide along with the application. The license key will be e-mailed to you upon the receipt of your payment.

1.3.1. License Agreement

License Agreement is a legal contract between you and Kaspersky Lab Ltd., which contains the terms and conditions, on which you may use the anti-virus product you have purchased.

Read the License Agreement carefully!

If you do not agree with the terms of the license agreement, you can return Kaspersky Anti-Virus to your dealer for a full refund. In this case, the envelope with the installation CD must remain sealed.

By opening the sealed envelope containing the installation CD or by installing the product on your computer you accept all terms and conditions of the License Agreement.

1.3.2. Registration card

Please provide your personal information on the detachable stab of the registration card: full name, phone number, e-mail address (if available) and send this stab to the dealer you purchased the product from.

If your mailing address, e-mail address or telephone number changed later, please notify the organization to which you mailed the registration card.

The registration card is a document that gives you the status of a registered user of Kaspersky Lab. This entitles you to receive support services during the period of your subscription. As a registered user, you may also subscribe to Kaspersky Lab Ltd. newsletter and receive updates about new releases of our products.

1.4. Services provided for registered users

Kaspersky Lab Ltd. offers to all legally registered users an extensive service package enabling them to use Kaspersky Anti-Virus more efficiently.

After purchasing a subscription, you become a registered user and, during the period of your subscription, you will be provided with the following services:

- you will be receiving new versions of the purchased software product;
- support on issues related to the installation, configuration and use of the purchased software product. Services will be provided by phone or via email;
- information about new Kaspersky Lab products and about new viruses appearing worldwide (this service is provided to users who subscribe to the Kaspersky Lab's newsletter).

Support on issues related to the performance and the use of operating systems or other technologies is not provided.

1.5. Conventions

Various formatting features and icons are used throughout this document depending on the purpose and the meaning of the text. The table below lists adopted conventions used in the text.

Format feature	Meaning/Usage
Bold font	Titles of menus, menu items, windows, dialog boxes and their elements, etc.
Note.	Additional information, notes
Attention!	Information requiring special attention
In order to perform 1. Step 1. 2. …	Description of the successive user's steps and possible actions
Task, example	Statement of a problem, example of the demonstration of the application's capabilities
Decision	Implementation of the task
[modifier] – modifier name.	Command line modifier
`Information messages and command line text`	Text of configuration files, information messages and command line

CHAPTER 2. INSTALLING THE APPLICATION

Before the installation of Kaspersky Anti-Virus make sure that the software and hardware of the computers used meet the installation requirements. The minimum allowable system configuration is described in section 1.2 on page 7.

For installation and removal of Kaspersky Anti-Virus 5.5 for Lotus Notes/Domino the local administrator's rights are required for the computer on which the installation is performed and the Lotus Notes/Domino administrator's rights.

2.1. Installing the application

The installation procedure is standard, similar to that of most Windows applications. The setup wizard will offer you to install the application components of Kaspersky Anti-Virus for Lotus Notes/Domino on the computer on which the setup wizard is run.

In order to install Kaspersky Anti-Virus into your computer run the executable file on the installation CD included into the distribution package. The installation process will be facilitated by the setup wizard. Setup wizard will offer you to configure the installation settings and start the installation. Following below is a detailed discussion of each step of the application installation.

The process of installation from a distribution kit received via internet is completely analogous to the installation from the installation CD.

Step 1. Verifying the version of the installed operating system

Before the application installation is started, a check will be performed to determine whether your operating system and the Service Packs installed meet the software requirements for the installation of Kaspersky Anti-Virus. If any of the required service packs for the operating system is not installed, perform the required updates and then reinstall Kaspersky Anti-Virus.

Additionally, if any other anti-virus software for Lotus Notes/Domino is installed on this computer, it may conflict with Kaspersky Anti-Virus 5.5. We recommend that you manually uninstall such software before proceeding with the installation.

Step 2. Greeting and License Agreement

First steps of the installation process are standard and involve unpacking the required files from the distribution kit and copying them to the hard drive of your computer. After this, a greeting window and a window containing the License Agreement will open. Read the text of the License Agreement carefully and accept terms and conditions contained therein to proceed with the installation.

Step 3. Entering user's information

During this step you will have to enter the required information in the User's information dialog box By default the dialog box will contain information obtained from the Windows register.

Step 4. Launching the installation process

After the settings are configured, launch the installation process. In order to do this, press the **Install** button. This will start the process of copying the application files to your computer.

Kaspersky Anti-Virus will be installed to the folder …\Program Files\Kaspersky Lab\Kaspersky Anti-Virus for Lotus Notes

Step 5. Installing license key

During this step Kaspersky Anti-Virus for Lotus Notes/Domino license key will be installed. The license key is your personal "key" that contains all service information required for the full-featured functionality of the application and additional reference information, namely:

- support information (who is providing support and how you can get help);
- restriction on the number of mail boxes;
- the license name, number and expiration date.

In the **Installed license keys** window that will open) press the **Add** button. Specify the license key file (*.key) to be installed in the standard Windows Select file dialog box. As the result, the selected license key will be installed as the license key for Kaspersky Anti-Virus.

If, at the time of the installation, you still do not have the license key (for example you ordered it from Kaspersky Lab via internet but have not received it yet), you can install it later when you run the application for the first time. Note that without the license key you cannot start using Kaspersky Anti-Virus.

Step 6. Completing the setup

After the installation is complete, press the **Finish** button in the final window of the setup wizard. Before you start using the application, you have to perform the post-installation setup (see section 2.2 on page 13).

Information about the installation process will be logged by the application in file **%TEMP%\kav_lotus.log**

2.2. Performing post-installation setup

In order to ensure that you application works correctly after the installation of Kaspersky Anti-Virus on the server has been completed, you must subscribe to the Domino server database as follows:

- Launch Domino Administrator.
- Select the servers on which Kaspersky Anti-Virus is installed from the list in the left frame of the window that will open.
- Switch to the **Files** tab.
- Select the Kaspersky Anti-Virus settings database (kldsettings.nsf) from the Lots databases list in the Files tab.
- Select the **Sign** command for this database from the mouse shortcut menu.
- Confirm the command by pressing the **OK** button in the window that will open.
- Close Domino Administrator.

Before the database subscription procedure, make sure that you have the Lotus Notes/Domino administrator's rights.

After the installation Kaspersky will start operating using the minimum set of parameters most of which are configured by default. However, if necessary, depending on the network properties and the characteristics of the computer, you can make all required changes and additions. In order to do this:

- Launch **Lotus Client**.
- Open **KavBases\klsettings.nsf**
- Make the required changes in the application's settings.

2.3. Removing the application

You can remove Kaspersky Anti-Virus for Lotus Notes/Domino from your computer using standard Windows Add/Remove Programs tool or the application distribution kit. This will remove all installed Kaspersky Anti-Virus components from your computer.

In order to uninstall Kaspersky Anti-Virus for Lotus Notes using the distribution kit:

1. Stop the Lotus Server.
2. Run the installation file from the installation CD. The removal process will be facilitated by the application service wizard. Follow its instructions.
3. Select the **Remove** option in the dialog box that will open.

If the Lotus Server was not stopped during the application removal, the process will not be performed correctly!

CHAPTER 3. KASPERSKY ANTI-VIRUS INTERNAL ARCHITECTURE

After the installation on the server Kaspersky Anti-Virus for Lotus Notes/Domino scans e-mail messages and Lotus Notes/Domino server databases for the presence of viruses and malicious objects. During its operation, the application uses the *anti-virus protection settings* that can be altered by an administrator, who knows the password required to access these settings, from any computer within the local network or remotely, using a program that opens in a web browser. Kaspersky Anti-Virus includes the following modules:

- **Hook** – e-mail messages interception module;
- **Kavmailmonitor** – e-mail messages scanning module;
- **Kavdbscanner** –Domino server database scanning module;
- **Replications monitor** – replications scanning module;
- **Kavupdater** – application anti-virus database updating module.

Additionally, the structure of the application includes a *virus outbreaks detection system*.

During its operation, the application uses several databases located on the server hard drive:

- Configuration database.
- Quarantine database.
- Statistical database and the application's run-time log.

Modules **Hook**, **Replications monitor, Kavupdater**, and scan modules **Kavmailmonitor** and **Kavdbscanner** start automatically at the Domino server startup, which is registered in the application's run-time log by entering the corresponding lines.

After the **Hook** module is started, it intercepts all e-mail messages sent by the Domino server (files *mail*.box*), and passes the messages to the **Kavmailmonitor** module for the anti-virus scan and processing.

The **Kavmailmonitor** module scans all received messages for viruses and processes these messages based on the configuration database anti-virus protection settings. For example, this module can attempt to disinfect all infected objects and place objects it failed to disinfect into the quarantine database. Additionally, the **Kavmailmonitor** module records its actions into the run-time log depending on the configuration database settings.

The **Kavdbscanner** module scans all Domino server databases using the current settings and processes them depending on the anti-virus protection settings. All functions and actions of this module are similar to the **Kavmailmonitor** module's functions.

The **Kavreplmonitor** module prevents the server infection by replicating documents from other Domino servers not protected by Kaspersky Anti-Virus. Local replications performed within one Domino server will not be scanned.

The detection system provides protection against virus outbreaks. Outbreak detection rules and criteria, as well as the possible actions to be performed once an outbreak is detected, can be determined through the configuration database by the administrator.

The Kavupdater module updates the anti-virus database used to detect and disinfect viruses.

If settings have been modified, the **Kavmailmonitor** and the **Kavdbscanner** modules will start operating using the new setting virtually right after the settings are saved into the configuration database. The **Hook** module will use new settings after the server is reloaded.

CHAPTER 4. CONFIGURING THE ANTI-VIRUS PROTECTION SYSTEM

All Domino server incoming/outgoing e-mail messages are scanned and processed by the **Kavmailmonitor** module and all server database files - by the **Kavdbscanner** module. Both modules use the anti-virus protection settings. These settings are included into the **Tasks Settings** and **Anti-Virus Kernel** groups in the configuration database window. Each group includes more specific tasks that reflect the functionality of the application. A detailed discussion of these tasks is provided below.

For convenience, the title of each section of this guide describing a particular window or a dialog box, includes the interface "path" to this window. For example, the title of the section that describes general settings of Kaspersky Anti-Virus operation will be as follows:

General settings of Kaspersky Anti-Virus operation. Tasks configuration/General, where **Tasks configuration/General** is the path to this window.

The settings displayed in any window can be modified as follows:

- Pressing the **Modify** button makes settings displayed in this window available for editing.
- If a setting configuration requires entering a certain value, such value will be provided in an entry field.
- If a setting can be modified by selecting one of the suggested options or by checking a box, the selection will be done using the selection button.

4.1. General settings of Kaspersky Anti-Virus operation. Tasks configuration/General

The **Tasks configuration/General window** (see Figure) displays the general operation settings of Kaspersky Anti-Virus for Lotus Notes/Domino:

- **Disinfect** – this box enables or disables the option of disinfecting infected objects detected.
- **Temporary folder** – full path to the temporary files folder used by Kaspersky Anti-Virus during the scan.
- **Administrators**– the list of users' e-mail addresses from which notifications will be sent.

You can access this window from the **Tasks configuration** section in the left frame of the main window of the configuration database by following the General hyperlink**.**

Figure 1. The General tab

4.2. Updates settings. Tasks configuration/Updates configuration

During the anti-virus scan and processing, the application uses the anti-virus database that can be configured in the **Tasks configuration/Updates configuration** window (see Figure 2). You can access this window from the **Tasks configuration** section located in the left frame of the main window of the configuration database by following the Updates configuration hyperlink**.**

You can perform the following tasks by modifying the settings of the anti-virus database updating process:

- Specify the database storage folders (main and backup folders).
- The backup folder is used to save the previous version of the anti-virus database that allows you to restore the database in case of a copying process failure.
- Specify the storage folder for temporary files used by the **Kavupdater** module.
- Select anti-virus database to be used during the scan:

  Standard database – anti-virus database that contains detailed description of all viruses existing at the moment and methods used for their detection and disinfection. This type of anti-virus database is used by default.

  Extended database – anti-virus database that, in addition to information about viruses, contains information about Riskware. Such programs contain vulnerabilities that can be used for hackers' attacks, installation of unauthorized software, etc.

  Redundant database – the most complete type of anti-virus database. In addition to information described above, this database also includes description of SpyWare and AdWare.

  SpyWare programs are used to get an unauthorized access to your personal information (for example, addresses of websites that you visited, passwords, banking information) and to send it to the intruders.

  AdWare programs are installed together with some other software and then display some advertising messages, open pop-up windows containing advertising information or force the user to visit the advertiser's website. Apart from forced advertising, such programs impose a considerable additional load on the communication channels and increase the traffic.

  If you use extended or redundant anti-virus database Kaspersky Anti-Virus may trigger “false alarms” in some cases when you download software used to increase the security level of your computer. For example, it can be remote surveillance programs that do not have their own installers.

  For regular operation mode it is sufficient to select standard anti-virus database. Extended and redundant anti-virus databases are used to ensure a higher information protection level. The use of more complete sets of anti-virus database increases the consumption of resources during the scan.

- Specify the sources of updates and database downloading settings.

Specify the source of updates from which the updates will be installed in the **Updates Source** section. The following resources can be used as the updates source:

- **HTTP-, FTP-server or a network folder** – a local server or folder where the administrator copies the updates downloaded from the internet. Specify the path to the folder in the **Local folder** entry field using the **Change** button.

If you selected the option of performing the updates from the HTTP, FTP server or a network folder, you must specify the connection protocol to be used when specifying the server or folder address.

When you define the address of the proxy server, the connection protocol does not have to be specified.

- **Kaspersky Lab's update servers** – Kaspersky Lab's HTTP-, FTP- internet servers, to which new updates are uploaded on a daily basis.

- Schedule the updates frequency. In order to do this, specify the frequency of copying the anti-virus database in the **Schedule** section:

  - **By days** – daily updates at a certain time of the day.
  - **By hours** – updates are performed at a certain time with the interval in hours specified by the user.

In addition, the administrator can start *on-demand anti-virus database update.* In order to do this, specify the required time for copying new database in the Next update date field of the **Downloading settings** using the format <**date> <time>**.

The correctness of these settings is of great importance. This is related to the fact that using up-to-date anti-virus database is one of the major factors affecting the quality of detection of infected objects by the Anti-Virus. Anti-virus scan and disinfection of infected objects are performed based on the records of the anti-virus database that contains description of all currently known viruses and methods used for the disinfection of objects infected with these viruses.

Kaspersky Lab adds information about new viruses to its anti-virus database and publishes the updated database version in the internet on an hourly basis. We recommend that you download updates *hourly*.

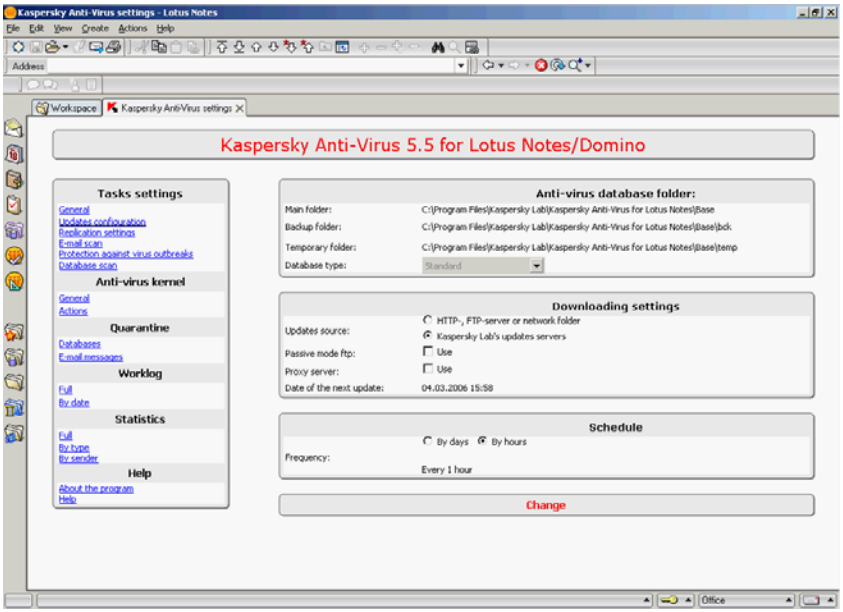

Figure 2. The Updates configuration tab

4.3. Replications scan settings. Tasks configuration/ Replications configuration

The replication process may involve moving certain files without the use of the system mailbox. This may result in the infection of the server protected by Kaspersky Anti-Virus. In order to prevent such situations, the application performs anti-virus scanning of all replications performed. The scan parameters are configured in the **Tasks configuration/Replications configuration** window (see Figure 3). You can access this window from the **Tasks configuration** section located in the left frame of the main window of the configuration database by following the Replications configuration hyperlink**.**

By configuring the scan settings you can:

- Specify the objects to be scanned. The following objects can be selected for scanning:

- **Attached objects** – scan all files attached to e-mail messages. By default, all attached files will be scanned for viruses.
- **Message body** – scan the body of the message.
- **OLE objects** – scan for viruses all OLE objects attached to the message.

- You can exclude certain types of objects from the scan scope using the **Filter by type** setting.

  In order to decrease the server load, you can disable the scan of some file types. In order to do it, configure the filtering by type option.

  - **Files in Win32 Portable Executable format** – format of executable files for the Win32 platform.
  - **Graphical files** – graphic files of **gif**, **bmp**, **jpg** and other formats.
  - **Multimedia files** – multimedia files of **wma**, **jpeg**, **mp3** and other formats.
  - **Other executable files –** files of **bas**, **bat**, **cmd**, **com**, **hta**, **jse**, **pcd**, **pif**, **sh**, **scr**, **vb**, **vbs**, **wsh** formats. We do not recommend excluding these file types from the scan scope.
  - Other file formats – file formats **chm**, **crt**, **dll**, **doc**, **dot**, **hlp**, **xls**, **xlt**, **xla**, **reg**.

Actions performed with objects after filtering are configured in the **Anti-virus kernel / Actions** window on the **Block by type** tab.

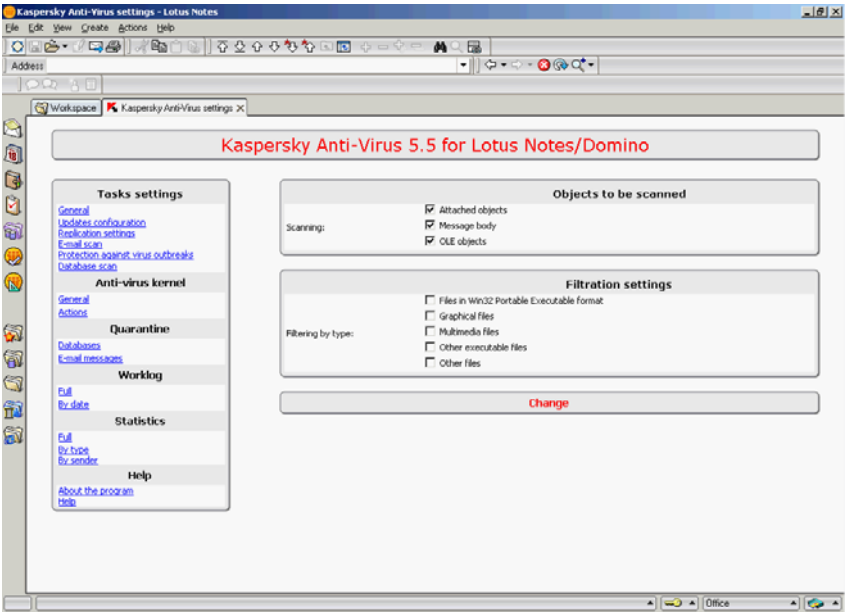

Figure 3. The **Replications configuration** tab

4.4. E-mail messages scan settings. Tasks configuration/E-mail scan

While scanning Domino server e-mail messages for viruses, the **Monitor** modules uses settings configured in the **Tasks configuration/E-mail scan** window (see Figure 4). You can access this window from the **Tasks configuration** section located in the left frame of the configuration database window by following the E-mail scan hyperlink**.**

By configuring the e-mail scan settings you can:

- Specify the object types to be scanned (in a similar way as described in section 4.3 on page 21).
- Specify the filtering mode to exclude certain objects from the scan scope. The following modes can be used:
    - **Filtering by size** – do not scan objects with size that exceeds a specified value. If the size of the attached object exceeds the

value specified in the settings, Kaspersky Anti-Virus will process it using the settings configured in the **Anti-virus kernel / Actions** window on the **Block by size** tab.

- **Filtering by type** – do not scan objects of a certain type (details about filtering settings see section 4.3 on page 21).

- Specify whether the original e-mail messages can be saved in the quarantine database.

The e-mail scan settings configuration process can be divided into two stages: first you have to specify the objects types to be scanned, and then - specify the scan settings.

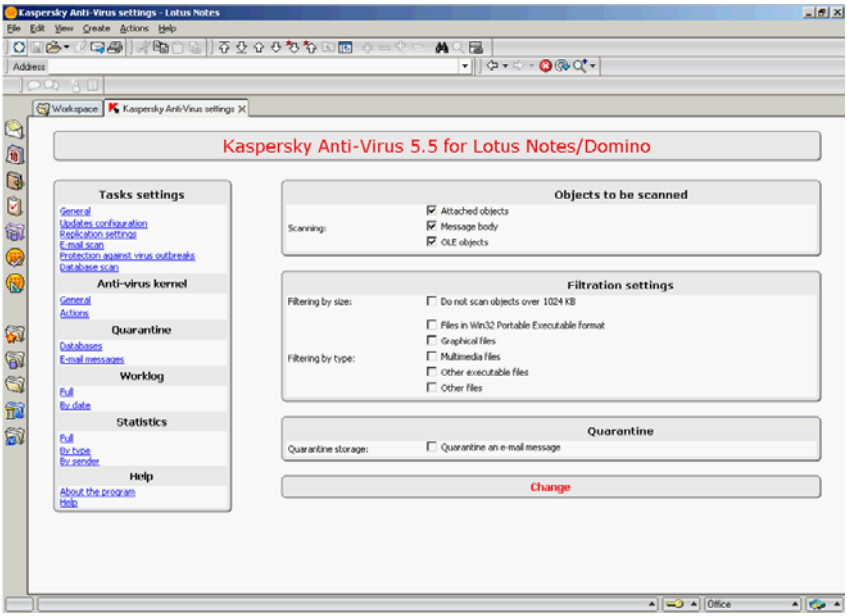

Figure 4. The **E-mail scan** tab

4.5. Anti-virus protection settings. Tasks configuration/Protection against virus outbreaks

Kaspersky Ant-Virus allows detecting increases in the virus activities on the protected Domino server and notifying the administrator and other users about such events. This feature is of great significance in the periods of virus outbreaks as it helps the administrator timely react on the emerging threats of virus attacks.

When detecting a virus outbreak, the **Monitor** module uses the settings specified in the **Tasks configuration/Protection against virus outbreaks** window (see Figure 5). You can access this window from the **Tasks configuration** section located in the left frame of the main window of the configuration database by following the Protection against virus outbreaks configuration hyperlink**.**

Virus activity level is determined based on the server anti-virus protection data and allows registering events of the following types:

- **An infected object detected**
- **A suspicious object detected**
- **A corrupted object detected**
- **One and the same virus detected several times.**

The administrator specifies the **virus activity level threshold** – a maximum allowable number of events of the specified type within a certain limited time interval. If the virus activity level exceeds the specified threshold, a notification about a new virus outbreak threat will be issued.

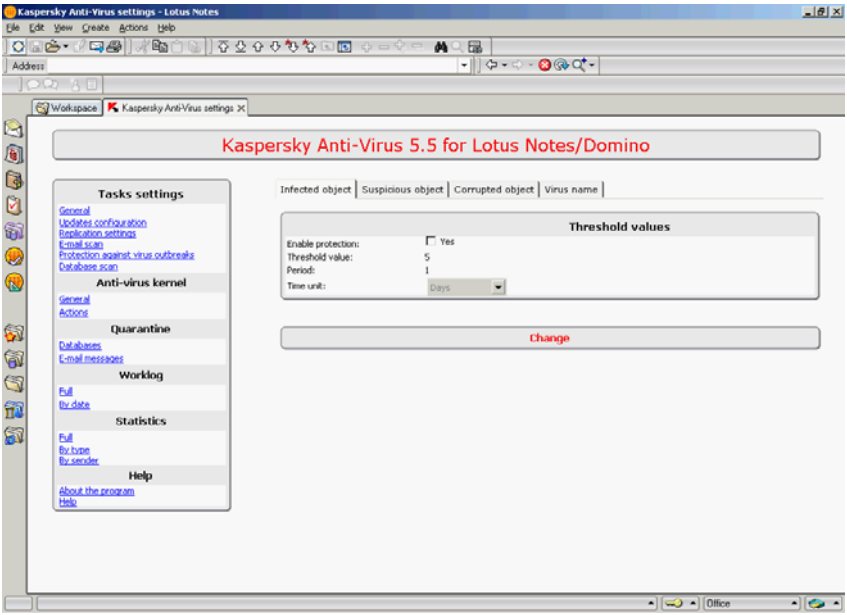

Figure 5. The **Protection against virus outbreaks** tab

4.6. Database scan settings. Tasks configuration/Database scan

When scanning the Domino server database files, the **Scanner** module uses settings specified in the **Tasks configuration/Database scan** window. You can access this window from the **Tasks configuration** section of the main window of the configuration database by following the Database scan hyperlink (see Figure 6)**.**

By configuring the database scan settings you can:

- Specify the objects to be scanned.
- Specify masks and include subfolders into the list of objects to be scanned.

When entering the database file masks, keep in mind that the names are case sensitive!

- Specify the objects to be excluded from the scan scope.

We recommend excluding the quarantine database from the scan scope. In order to do it, specify path to the quarantine database from the Domino Data folder in the **Exclusions** field. When entering the path, note that it is case-sensitive.

- Schedule the updates frequency.

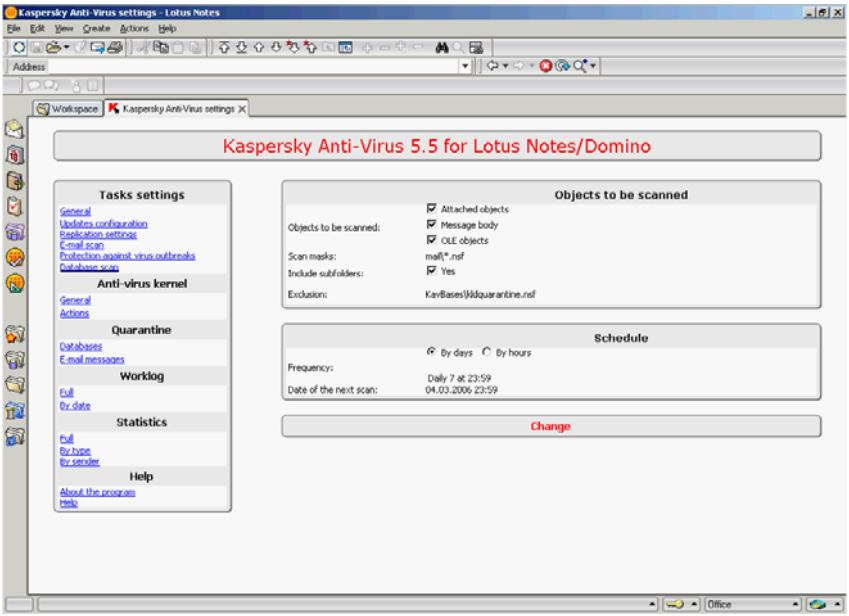

Figure 6. The **Database scan** tab

4.7. Anti-virus protection settings. The *Anti-virus kernel* section

Since Kaspersky Anti-Virus for Lotus Notes/Domino allows scanning the Domino server database files, in addition to e-mail messages, both e-mail messages and database files will be subject to scanning.

For example, an infected object may be a file attached to a e-mail message or an OLE object of a database file, however all these objects will be processed using the same settings that have been assigned for infected objects processing in the configuration database.

In order to configure the anti-virus protection settings, the user will have to determine which objects types will be scanned and to assign certain actions to be performed by Kaspersky Anti-Virus in case of detecting objects with certain statuses.

4.7.1. Anti-virus kernel/General

During the its operation, Kaspersky Anti-Virus uses anti-virus protection settings specified in the **Anti-virus kernel/General window**. You can access this window from the **Anti-virus kernel** section located in the left frame of the main window of the configuration database by following the General hyperlink (see Figure 7)**.**

By configuring the scan settings you can:

- Set the anti-virus scan for objects of the following types:
  - Archives
  - Packed executable files
- Enable/disable the heuristic code analyzer (redundant scan). The heuristic code analyzer performs the analysis of the sequence of commands in the object being scanned using a statistics data set. This facility is used for detecting viruses that are not known yet.

The use of heuristic analyzer may lead to incorrect scan of some types of objects. In this case, after the scan such objects will be assigned the **Not scanned due to a failure** status. We recommend that you do not set the **Delete** action as the default action for objects with this status.

- Specify the anti-virus kernel response timeout.

- Specify the number of instances of the anti-virus kernels that can run simultaneously.

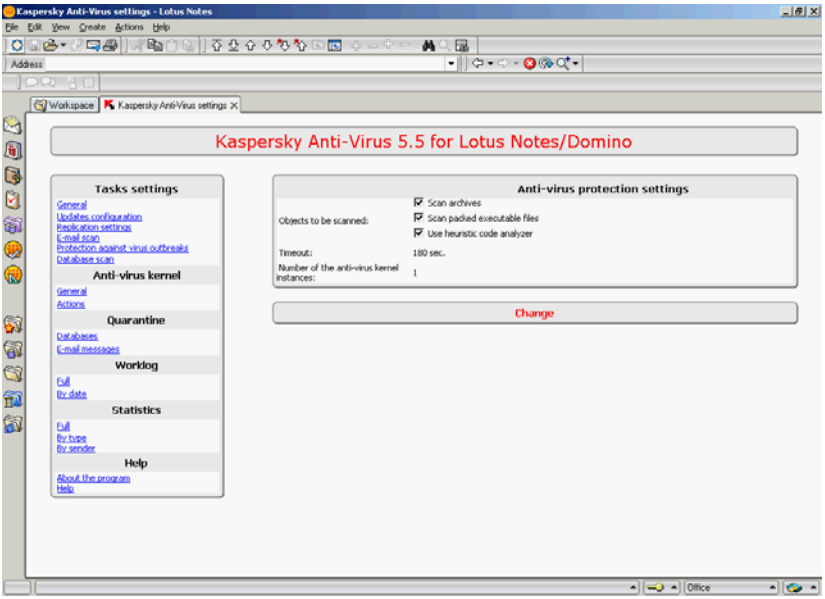

Figure 7. The **General** tab

4.7.2. Anti-virus kernel/Actions

The processing of objects are performed by the anti-virus kernel. As the result of anti-virus scan and processing, each object can be assigned a status from the list below:

- **Not infected** – object does not contain viruses.
- **Disinfected** – infected object that was successfully disinfected.
- **Infected** – object contains one of known viruses.
- **Suspicious** – object's code is similar to the code of a known or an unknown virus.
- **Corrupted**– object is corrupted.
- **Not scanned –** object cannot be scanned (for example, this object is password-protected).

- **Not scanned due to an error** – object has not been scanned due to a system error (for example, no right to access the object).
- **Block by type** – object has not been scanned because the configuration database settings do not provide for the anti-virus scan and processing of this type of objects.

Kaspersky Anti-Virus does not scan encrypted objects.

An object can be processed using certain actions depending on its status. The processing settings are available on the kernel status tabs in the **Anti-virus kernel/Actions** window. You can access this window from the **Anti-virus kernel** section located in the left frame of the main window of the configuration database by following the Actions hyperlink (see Figure 8)**.**

The most important major function of the application is the disinfection of **infected** objects. Disinfection is performed based on the information contained in the anti-virus database. According to the results of the attempted disinfection, an object can be assigned a status as listed below:

The following actions are provided for to be performed with the objects with the following statuses: **Infected, Suspicious, Corrupted, Not scanned, Skipped, Not scanned due to an error, Block by type:**

- **Skip** – skip the object, do not make changes;
- **Delete** – delete objects with this status.

Before the processing, a copy of the object can be saved in the quarantine storage to be restored later.

The application can send notifications about detected objects to the administrator and other users or register such events in the statistical information database.

For objects with the **Disinfected** status, Kaspersky Anti-Virus automatically replaces the infected object with its copy that has been disinfected and allows saving a copy of the original object into the quarantine storage with a notification to specified recipients.

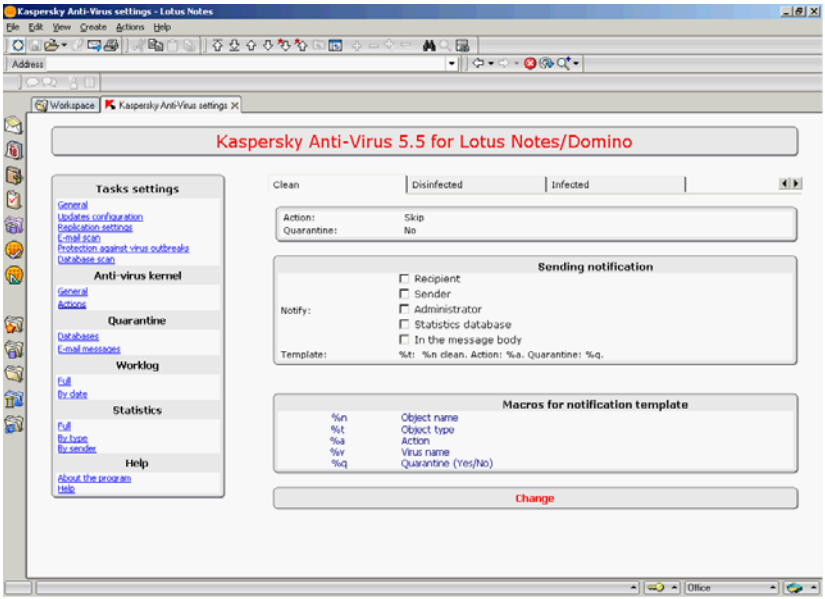

Figure 8. The **Actions** tab

4.7.3. Notifications

Kaspersky Anti-Virus includes the feature of notifying about objects of certain statuses detected during the scan. In order to enable this feature, check the corresponding box on the kernel status tab **Sending notifications** section of the **Anti-virus kernel/Actions** window. Notifications can be sent to:

- Server administrator (if an object of a certain status is detected either in an e-mail message or in a database);
- The sender of the e-mail message;
- The recipient of the e-mail message;

In addition, the application can save data about detecting objects in the statistical database.

Notifications can be sent as separate messages and can be added to the body of the mail message using the **In the message body** option.

If you need to add a notification to a message in the MIME format, it will be converted into a Rich Text format message.

The notification procedure and the text of messages to be sent are defined by the administrator as notification templates. Based on a template, if an event of a certain type happened, a notification about such event will be performed.

A type of the notification template created is displayed in the **Template** line of the **Anti-Virus kernel/Actions** window. When creating a template you can use macro substitution by selecting required entries from the Macros for notification templates list.

CHAPTER 5. ADDITIONAL SETTINGS

The following databases are used by Kaspersky Anti-Virus for Lotus Notes/Domino during its operation:

- **Quarantine database for:**
    - **E-mail messages** – a database of e-mail attachment objects quarantined for further processing.
    - **Databases** – database of documents quarantined after being scanned by the **Scanner** module.
- **Worklog** – database that stores reports about the results of operation of the **Monitor** and the **Scanner** modules for each processed object.
- **Statistics** –database that stores results of the anti-virus scan of each object.

For convenience, the title of each section of this guide describing a particular database includes the interface "path" to this database. For example, a section that contains a description of the scan database is referred to as follows:

> **Working with objects in the quarantine database. Quarantine/Databases**,
>
> where **Quarantine/Databases i**s the path to the window that displays the quarantine database **(Quarantine** is a section in the left frame of the window of the configuration database, **Databases** is a hyperlink you have to follow in order to access this window).

5.1. Quarantine database

Kaspersky Anti-Virus for Lotus Notes/Domino offers an ability to save objects with a certain status in the quarantine database.

This can be useful if the object is infected and cannot be disinfected at this moment. However, if this object contains valuable information, we recommend placing it into the quarantine database and later – scanning it again using an updated anti-virus database.

Option used for quarantining objects is configured in the **Anti-Virus kernel/Actions** section on the corresponding tabs of the object status (details about object status see 4.7.2 on page 29).

If you selected the **Quarantine** action as the action to be performed with objects having the **Disinfected** status, the application will quarantine the disinfected object rather than the original object.

Any data in the quarantine database is divided into e-mail message objects and Domino server database files.

- Database files quarantine – a section in the quarantine database that stores Domino server database objects being scanned.
- E-mail messages quarantine - a section in the quarantine database that stores e-mail message objects.

The titles of the quarantine database sections are displayed in the **Quarantine** section located in the left frame of the configuration database window. The name of each section is displayed as a hyperlink used to update the dynamic right frame of the window. Later an object stored in the quarantined database can be sent to the recipients or deleted.

5.1.1. Working with documents in the quarantine database. Quarantine database/Databases

In order to access the quarantine database of the Domino server database objects, follow the Databases hyperlink located in the **Databases** section in the left frame of the configuration database window (see Figure 9). As the result the right frame of the window will be updated to display the list of documents quarantined after the scan.

The right frame is formatted as a table that contains the following information:

- **Server** – the name of the protected server.
- **Database** – the name of the database containing the quarantined object.
- **Modified** – information about all users who modified the quarantined document.

This section will also contain information about the name of the quarantined object.

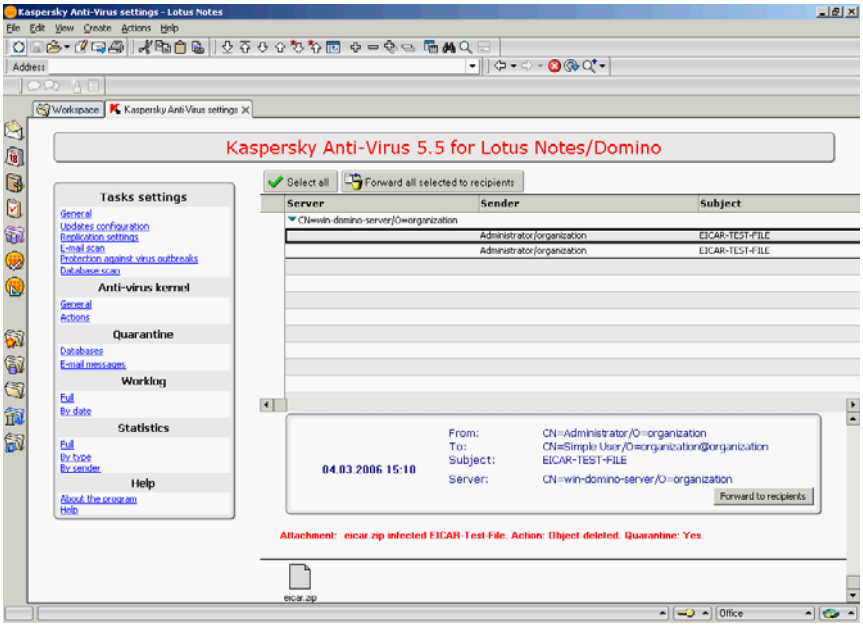

Figure 9. The **Database quarantine** tab

If an object is moved to the quarantine storage, it will be stored until it is deleted by the administrator. Therefore we recommend that you periodically delete objects that do not contain valuable information from the quarantine folder.

In order to manually delete an object from the quarantine storage:

- Select the object you wish to delete in the table that displays the quarantine content.
- Open the shortcut menu and use the **Delete** command or a similar item in the **Edit** menu.

As the result the object will be deleted from the quarantine folder.

5.1.2. Working with e-mail message objects in the quarantine database. Quarantine/E-mail messages

In order to access the quarantine database, follow the E-mail messages hyperlink, located in the **Quarantine** section of the left frame of the configuration database window (see Figure 10).

The right frame is formatted as a table that contains the following information:

- **Server** – the name of the protected server.
- **Sender** – address of the sender of the quarantined e-mail message object.
- **Subject** – the subject of the message.

Any e-mail message object in the quarantine database is a document that contains the following scan results:

- **Sender** – address of the sender of the quarantined e-mail message object.
- **Recipients** – address of the recipients of the e-mail message.
- **Subject** – the subject of the message.
- **Server** – the name of the protected server.
- **Attachment** – the original name of the attached object and the results of its scan by the Anti-Virus.

Sometimes a message may contain several attached objects with the same name.

In this case, when the scan results are displayed, the original name will only be saved for one of the attachments while for others their unique system names will be displayed.

- **Return code** – the verdict of the anti-virus kernel after the scan of the object (infected, clean, etc.)
- **Action** – settings used for object processing.

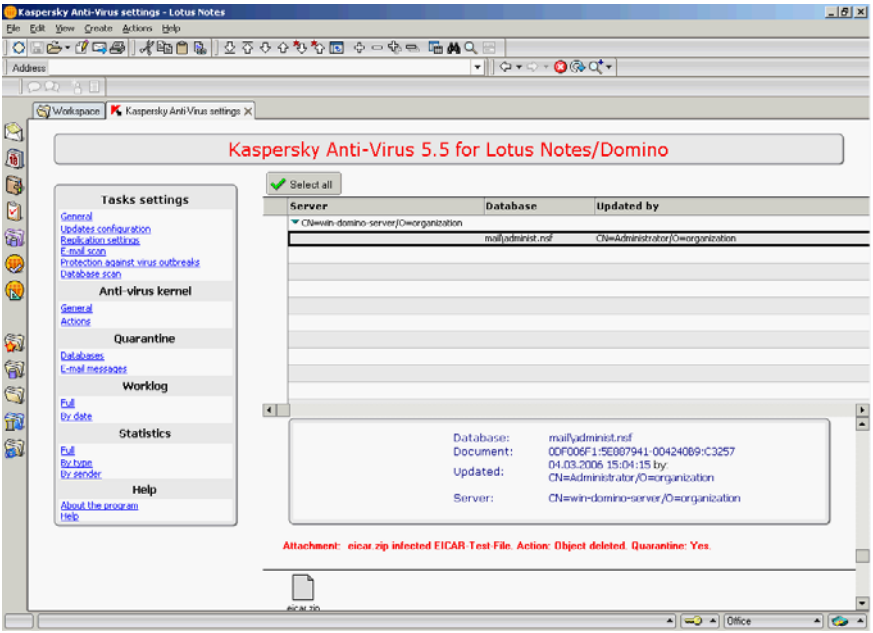

Figure 10. **E-mail messages quarantine** tab

Later an e-mail from the quarantine can be:

- **Send to the recipients** so that they can receive information contained in the message. Besides, you can restore the infected object and rescan it with the file anti-virus using the up-to-date anti-virus database.
- **Deleted.** E-mail messages deletion is performed alike the procedure used to delete objects from the database quarantine folder (details see section 5.1.1 on page 34).

In order to restore an e-mail message from the quarantine:

- Select the object you wish to restore in the table displaying the storage content.
- Press the **Forward to recipients** button.

Before you send the message a warning message will be displayed prompting your confirm the operation. In order to restore the file from the quarantine, press the **OK** button.

As the result, the object will be sent from the quarantine storage to the specified recipient.

5.2. Worklog

The key results of the **Kavmailmonitor** and the **Kavdbscanner** modules are registered in the application's worklog (see Figure 11). All records about the results of the modules' operation are grouped as detailed below:

- Full – list of records grouped by the record creation date.
- By date – list of records grouped by the information contained. The information contained in the records may be of the following types:
    - **Information** – informational message;
    - **Warning** – a notification of an event.

The list of groups of records is located in the **Worklog** section in the left frame of the configuration database window. The name of each group is displayed as a hyperlink used to update the dynamic right frame of the window.

The structure of the right frame for each type of grouping of the worklog records is a table with the following columns:

- **Date** – worklog record creation date.
- **Time** – worklog record creation time.
- **Server** – the name of the server on which the task is performed.
- **Task** – the name of the module, the results of which operation are registered.
- **Description –** a full description of the results of the module's operation.

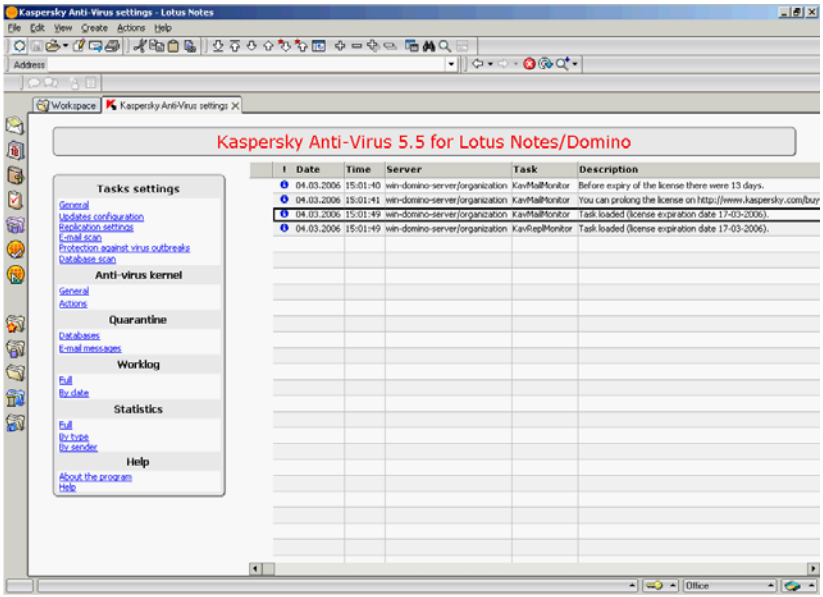

Figure 11. Worklog

5.3. Anti-virus statistics

The results of the anti-virus objects scan are registered in the application's anti-virus statistics log (see Figure 12). All records about the results of the operation are grouped as detailed below:

- Full – list of records grouped by the record creation date.
- By type – list of records grouped by the status of the scanned objects.
- By sender – list of records grouped by the sender's address (for e-mail messages only).

The list of groups of records is located in the **Statistics** section in the left frame of the configuration database window. The name of each group is displayed as a hyperlink used to update the dynamic right frame of the window.

The structure of the right frame for any type of records grouping in the statistics database is similar to the structure of the records in the worklog. The right frame displays the following information:

- An icon that reflects the current status of the object.

- **Date** – database record creation date.
- **Time** – database record creation time.
- **Server** – the name of the server on which the task is performed.
- **Task** – the name of the module, the results of which operation are registered.
- **Description –** results of the anti-virus scan, namely, the virus name, if the object is infected.

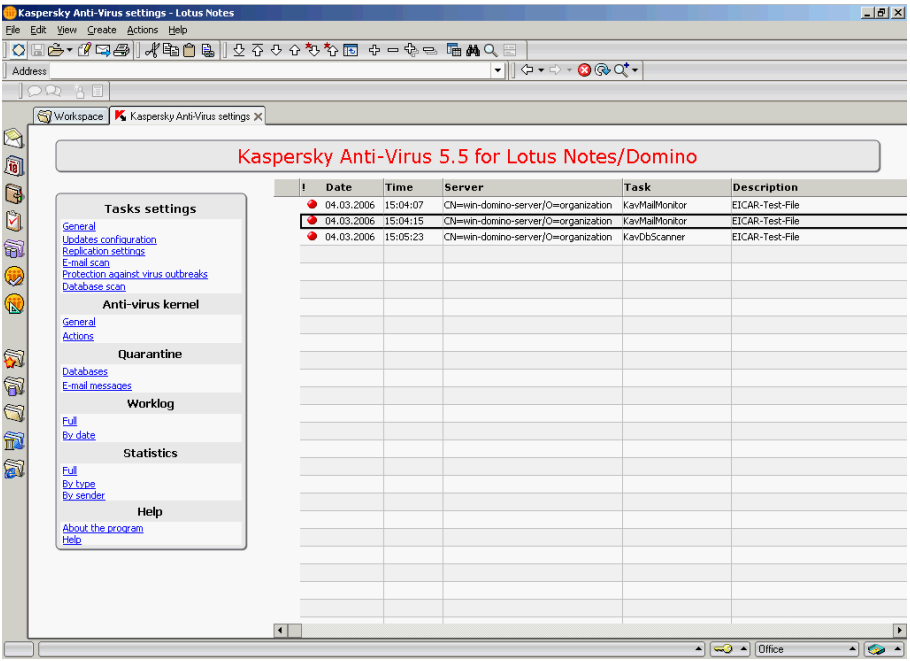

Figure 12. Anti-Virus Statistics

Please note that the option of notifying the statistics database about detection of an object of a certain status is specified on the **Actions** tab of the **Anti-virus kernel** group of the configuration database!

5.4. Working with license keys

Kaspersky Anti-Virus 5.5 for Lotus Notes/Domino provides for the restriction of using the application based on the time period of its usage (as a rule, one year since the date it was purchased). After the expiration of the license, Kaspersky Anti-Virus will continue operating, but the anti-virus database updating feature will not be available. The anti-virus application will continue disinfecting objects infected with viruses but it will be using old anti-virus database.

5.4.1. Managing license keys

License key gives you the right to use the application and contains all necessary information related to the license that you have purchased, such as: license type, license expiration date, dealer's details, etc.

The following features will be available for you during the license period:

- using the anti-virus functionality of the application;
- *hourly* anti-virus database update;
- application updates (patches);
- receiving new versions of the application (upgrades);
- support on issues related to the installation, configuration and the use of the purchased software product, provided 24 hours a day by phone or via email;
- ability to send infected and suspicious objects to Kaspersky Lab for expert analysis.

The application verifies the validity of the license agreement by the **license key** that is an integral part of any Kaspersky Lab's product.

Kaspersky Anti-Virus WILL NOT WORK without a license key!

An application can use only one active license key. This license key contains restrictions imposed on the use of Kaspersky Anti-Virus that can be verified by the special application's utilities.

Two weeks prior to the license expiration date you will receive a warning message (when the application is running). This message contains information about the expiration date of the currently **installed license key**.

We recommend that you timely renew your license for using Kaspersky Anti-Virus.

5.4.2. Renewing your license

Renewal of your Kaspersky Anti-Virus item gives you the right for to restore the full-featured functionality of the application. Besides, additional services listed in section 5.4.1 on page 41 have been resumed.

Kaspersky Lab Ltd. periodically announces campaigns that allow you to enjoy considerable discounts when you renew you license for the use of our products. In order to keep informed about our offers visit Kaspersky Lab's corporate website and go to **Products → Sales and special offers**

In order to renew your Kaspersky Anti-Virus license,

Contact the dealer you originally purchased the product from and buy a new license key for the use of Kaspersky Anti-Virus 5.5 for Lotus Notes/Domino.

or:

Purchase a new license key directly from Kaspersky Labs. In order to do this, send a request directly to our Sales Department (sales@kaspersky.com) or fill out a form at our website (http://www.kaspersky.com). Upon the receipt of your payment, we will send a new license key to the e-mail address specified in your order.

The license key that you have purchased must be installed using the **Monitor** module.

In order to install a new key:

1. Stop the **kavmonitor** module. In order to do this enter in the command line:

```
tell kavmailmonitor quit
```

2. Start the license key installation procedure. In order to do this enter in the command line:

```
load kavmailmonitor <full_path_to_the_key_file>
```

The license key must be copied to the server before the installation.

Information about the license key is displayed at the application startup. You can also view this information by running a special task from the command line (details see section 5.5 on page 43).

5.5. Managing the application using command line

Some of the application tasks are easier to be performed using the command line options. Provided below is a detailed discussion of these tasks.The syntax of any of commands you enter shall be as follows:

```
tell <task_name> <line>
where:
task_name – the name of the module that performs the particular task;
line – system command.
```

In order to view the version of the application installed on the server, enter the following in the command line:

```
tell kavmonitor version
```

In order to view the serial number of the license key installed and the number of licenses, enter the following in the command line:

```
tell kavmonitor keyinfo
```

In order to launch an on-demand file system scan, enter the following in the command line:

```
tell kavdbscanner start
```

In order to stop the on-demand file system scan, enter the following in the command line:

```
tell kavdbscanner stop
```

In order to view the time when the next anti-virus database scan will be launched, enter the following in the command line:

```
tell <kavdbscanner> <shownext>
```

In order to delete information about the results of the previous database scans, enter the following in the command line:

```
tell <kavdbscanner> <rlsd>
```

In order to launch an on-demand anti-virus database update, enter the following in the command line:

```
tell <kavupdater> <start>
```

In order to view the time when the next anti-virus database update process will be launched, enter the following in the command line:

```
tell <kavupdater> <shownext>
```

It is recommended not to use **tell kavmailmonitor quit** command to stopping E-mail scanning. Mail delivery from the Lotus Notes\Domino server will be blocked as the result of this command.

CHAPTER 6. VERIFYING THE APPLICATON'S OPERATION

After Kaspersky Anti-Virus is installed and configured, we recommend verifying the correctness of its settings, operation and the correct creation of the message scan stamps using a test "virus" and its modifications.

This test "virus" was specially designed by eicar (The European Institute for Computer Antivirus Research) for testing anti-virus products.

The test “virus” IS NOT A VIRUS because it does not contain code that can harm your computer. However, most anti-virus products manufacturers identify this file as a virus.

Never use real viruses for testing the operation of an anti-virus product!

You can download test "virus" from the official website of **EICAR**: http://www.eicar.org/anti_virus_test_file.htm. If you have no Internet connection, you can create your own test "virus". To create a test “virus,” type the following in any text editor and save the file as **eicar.com**:

X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*

The file downloaded from the **EICAR** website or created as described above contains the body of a standard test “virus”. Kaspersky Anti-Virus will detect it, assign to it the **Object infected,** not disinfectable type and apply the action defined by the administrator for processing objects of this type.

To test the response of Kaspersky Anti-Virus when other types of objects are detected, you can modify the content of this standard test “virus” by adding one of the prefixes (see Table 1).

Table 1. Modifying the test "virus"

Prefix	Object status
No prefix, standard test virus	**Object infected**. Objects will not be disinfected.

Prefix	Object status
CORP–	Unidentified.
SUSP–	**Suspicious** (Code of an unknown virus).
WARN–	**Suspicious** (Modified code of a known virus).
ERRO–	**Object causes scan error,** that corresponds to the detection of a corrupted object
CURE–	**Object disinfected.** The object is disinfected; the text of the “virus” body will be replaced with the word "CURED"
DELE–	Objects will be automatically deleted.

The first table column lists prefixes to be added at the beginning of the string of the standard test “virus” (for example, CORR–X5O!P%@AP[4\PZX54(P^)7CC)7}$EICAR-STANDARD-ANTIVIRUS-TEST-FILE!$H+H*). The second column of this table contains the types of objects identified by Kaspersky Anti-Virus application after you have added a prefix. Actions to be performed with each object are determined by the Kaspersky Anti-Virus settings specified by the administrator.

We recommend that you test how Kaspersky Anti-Virus handles incoming and outgoing e-mail messages including both the body of the message and the attachments. In order to test detection of viruses in the body of the message, copy the text of the standard or of the modified test "virus" into the body of the message.

APPENDIX A. FREQUENTLY ASKED QUESTIONS

This chapter is devoted to questions most frequently asked by users regarding the installation, setup, and operation of Kaspersky Anti-Virus. We will try to answer them here in detail.

Question: Why does Kaspersky Anti-Virus® cause a certain decrease in my computer performance and impose a considerable load on the processor?

The process of virus detection is a purely computational (mathematical) task that involves analysis of structures, checksum calculation and mathematical data transformation. Therefore, the main resource consumed by the anti-virus software is the processor time. Moreover, each new virus added into the anti-virus database adds to the overall scanning time. This is the price that computer users pay for the security of their data.

Unlike other anti-virus software vendors that speed up the scan process by excluding from their databases viruses that are less easily detectable or less frequent in the geographic location of the anti-virus vendor and file formats that require complicated analysis (e.g. PDF files), Kaspersky Lab believes that the purpose of an anti-virus program is to deliver to its users a genuine anti-virus security rather than the illusory sense of safety, since you cannot be "half-protected". Besides, being "half-protected" is even worse than having no protection at all, as in the latter case many users resort to their own "home-grown" safety measures.

Users of Kaspersky Anti-Virus have all reasons to feel that they have maximum protection. Of course, Kaspersky Anti-Virus allows experienced users to accelerate the anti-virus scanning process to the detriment of the overall security by disabling scanning of various file types, but we do not recommend doing so to users, who want the best possible protection.

Question: After the Anti-Virus is installed, my mail is accumulating in the intermediate mailbox, but is not getting scanned. Why does it happen?

Make sure that the *kavmonitor* module started after you installed the application. In order to do this, enter from the Domino console in the command line:

```
show tasks
```

Look for the *kavmonitor* module in the task list that will appear on your screen. If this task is missing, try to launch it manually by entering:

```
load kavmailmonitor
```

If the task has not launched after this, send a message to the technical support service indicating the error code.

Question: Why do I need a license key? Will my Anti-Virus work without it?

Kaspersky Anti-Virus will not work without a license key.

If you are still undecided whether or not to purchase Kaspersky Anti-Virus, we can provide you with a temporary key file (trial key), which will only work either for two weeks or for a month. When this period expires, the key will be blocked.

Question: What happens when my Kaspersky Anti-Virus license expires?

When your Kaspersky Anti-Virus expires, your program will cease to update the anti-virus database.

Question: The settings are selected so that infected objects attached to the mail message are deleted. However, messages are still delivered with the attached file. Why.

The architecture of Lotus Notes/Domino does not allow deletion of the entire attached file. However, if the administrator selected deletion of infected attached objects in the settings of Kaspersky Anti-Virus, any infected attachment will be replaced with an attachment template. Attachment template is a text file kavdummy.txt included in the application distribution kit.

Question: My Anti-Virus does not work.

What should I do?

We recommend that you contact the dealer you purchased Kaspersky Anti-virus from or send a message to the technical support service (support@kaspersky.com).

To ensure that your request is answered as soon as possible, follow the below suggestions:

Specify the operating system installed on your server, the name of the component you cannot configure and indicate the problem in the subject of your message.

At the beginning of you message, specify the exact version of your operating system, Kaspersky Anti-Virus distribution package details, your license key information and the exact version of Lotus Domino installed on your server.

Briefly, but clearly describe the problem. Bear in mind that the support specialists had no previous knowledge of your problem and can only help you if they fully understand it and have been able to reproduce it.

Forward to the technical support service the following data packed in one archive:

- Kaspersky Anti-Virus report file;
- your license key.

Indicate the approximate daily mail traffic and load peaks if applicable.

Question: Can an intruder replace my anti-virus database?

An intruder can download the anti-virus database files from Kaspersky Lab's website and copy them into the folder that stores the anti-virus database used for your application, however, Kaspersky Anti-Virus will not use them in its operation!

All anti-virus databases are supplied with a unique signature verified by Kaspersky Anti-Virus when the program tries to use them. If the signature does not match with the signature assigned by Kaspersky Lab or it is stamped by a later date compared to your license expiry date, Kaspersky Anti-Virus will not use this database.

Question: Can Kaspersky Anti-Virus be used with other vendors' anti-virus software?

In order to avoid conflicts we recommend that you remove any third-party anti-virus software before you install Kaspersky Anti-Virus.

Question: Kaspersky Anti-Virus does not rescan file. Why?

In fact, Kaspersky Anti-Virus does not rescan file that have not been modified since the last scan.

This is possible due to the use of new technologies iChecker and iStreams. This technology is implemented by using the objects checksums database and storing the checksums of files in the additional NTFS streams

Question: Why hourly updates are required?

Several years ago viruses distributed via floppy disks and at that time it was sufficient to install an anti-virus program and update the anti-virus database from time to time to ensure adequate computer protection. Yet, the recent virus outbreaks spread over the world in a matter of several hours and anti-virus software using old anti-virus databases may not be able to protect you against a new threat. Therefore, to ensure protection against new viruses you have to update you anti-virus database on a hourly basis.

Kaspersky Lab shortens the anti-virus database update interval every year. Now the anti-virus database is updated every hour.

APPENDIX B. KASPERSKY LAB

Founded in 1997, Kaspersky Lab has become a recognized leader in information security technologies. It produces a wide range of data security software and delivers high-performance, comprehensive solutions to protect computers and networks against all types of malicious programs, unsolicited and unwanted email messages, and hacker attacks.

Kaspersky Lab is an international company. Headquartered in the Russian Federation, the company has representative offices in the United Kingdom, France, Germany, Japan, USA (CA), the Benelux countries, China and Poland. A new company department, the European Anti-Virus Research Centre, has recently been established in France. Kaspersky Lab's partner network incorporates more than 500 companies worldwide.

Today, Kaspersky Lab employs more than 250 specialists, each of whom is proficient in anti-virus technologies, with 9 of them holding M.B.A. degrees, 15 holding Ph.Ds, and two experts holding membership in the Computer Anti-Virus Researchers Organization (CARO).

Kaspersky Lab offers best-of-breed security solutions, based on its unique experience and knowledge, gained in over 14 years of fighting computer viruses. A thorough analysis of computer virus activities enables the company to deliver comprehensive protection from current and future threats. Resistance to future attacks is the basic policy implemented in all Kaspersky Lab's products. At all times, the company’s products remain at least one step ahead of many other vendors in delivering extensive anti-virus coverage for home users and corporate customers alike.

Years of hard work have made the company one of the top security software manufacturers. Kaspersky Lab was one of the first businesses of its kind to develop the highest standards for anti-virus defense. The company’s flagship product, Kaspersky Anti-Virus, provides full-scale protection for all tiers of a network, including workstations, file servers, mail systems, firewalls and Internet-gateways, hand-held computers. Its convenient and easy-to-use management tools ensure advanced automation for rapid virus protection across an enterprise. Many well-known manufacturers use the Kaspersky Anti-Virus kernel, including Nokia ICG (USA), F-Secure (Finland), Aladdin (Israel), Sybari (USA), G Data (Germany), Deerfield (USA), Alt-N (USA), Microworld (India) and BorderWare (Canada).

Kaspersky Lab's customers benefit from a wide range of additional services that ensure both stable operation of the company's products, and compliance with specific business requirements. Kaspersky Lab's anti-virus database is updated every 3 hours. The company provides its customers with a 24-hour technical

support service, which is available in several languages to accommodate its international clientele.

B.1. Other Kaspersky Lab Products

Kaspersky Anti-Virus® Personal

Kaspersky Anti-Virus ® Personal has been designed to provide anti-virus protection to personal computers running Windows 98/ME or Windows 2000/NT/XP against all known viruses, including potentially dangerous software. Kaspersky Anti-Virus Personal provides real-time monitoring of all sources of virus intrusion - e-mail, internet, CD, etc. The unique system of heuristic data analysis allows efficient processing of yet unknown viruses. This application can work in the following modes (that can be used separately or jointly):

- **Real-time computer protection** - anti-virus scanning of all objects run, opened on or saved to the user's computer.
- **On-demand computer scan** - scan and disinfection of the entire user's computer or of individual disks, files or folders. You can start such scan manually or configure an automatic scheduled scan.

Kaspersky Anti-Virus® Personal does not re-scan objects that had been already scan during a previous scan and have not changed since then not only when performing real-time protection, but also during an on-demand scan. This **considerably increases the speed of the program's operation**.

The application creates a reliable barrier to viruses when they attempt to intrude your computer via e-mail. Kaspersky Anti-Virus® Personal performs automatic scan and disinfection of all incoming and outgoing mail sent or received using POP3 and STMP protocol and provides highly efficient detection of viruses in mail databases.

The application support over 700 formats of archived and compressed files and provides automatic scan of their content as well as removal of malicious code from **ZIP, CAB, RAR, ARJ, LHA,** and **ICE** archives.

Configuring the application is made simple and intuitive due to the possibility to select of the preset protection levels: Maximum Protection, Recommended and High Speed.

The anti-virus database is updated every three hours and its delivery to your computer is guaranteed even when your computer gets temporarily disconnected from the internet or the connection has been changed.

Kaspersky Anti-Virus® Personal Pro

This package has been designed to deliver comprehensive anti-virus protection to home computers running Windows 98/ME/2000/NT/XP as well as MS Office 2000 applications. Kaspersky Anti-Virus Personal Pro includes an easy-to-use application for automatic retrieval of daily updates for the anti-virus database and the program modules. A second-generation heuristic analyzer efficiently detects unknown viruses. Kaspersky Anti-Virus Personal includes many interface enhancements, making it easier than ever to use the program.

Kaspersky Anti-Virus® Personal Pro has the following features:

- **On-demand scan** of local disks;
- **Real-time automatic protection** of all accessed files from viruses;
- **Mail Filter** automatically scans and disinfects all incoming and outgoing mail for any mail client that uses POP3 and SMTP protocols and effectively detects viruses in mail databases;
- **Behavior blocker** that provides maximum protection of MS Office applications from viruses;
- **Archive scans –** Kaspersky Anti-Virus recognizes over 700 formats of archived and compressed files and ensures automatic anti-virus scanning of their content and removal of malicious code from files within **ZIP**, **CAB**, **RAR, ARJ, LHA,** and **ICE** archives.

Kaspersky® Anti-Hacker

Kaspersky® Anti-Hacker is a personal firewall that is designed to safeguard a computer running any Windows operating system. It protects your computer against unauthorized access and external hacker attacks from either the Internet or the local network.

Kaspersky® Anti-Hacker monitors the TCP/IP network activity of all applications running on your machine. When it detects a suspicious action, the application blocks the suspicious application from accessing the network. This helps deliver enhanced privacy and 100% security of confidential data stored on your computer.

The product's SmartStealth™ technology prevents hackers from detecting your computer from the outside. In this stealthy mode, the application works seamlessly to keep your computer protected while you are on the Web. The application provides conventional transparency and accessibility of information.

- Kaspersky® Anti-Hacker also blocks most common network hacker attacks and monitors for attempts to scan computer ports.
- Configuration of the application is simply a matter of choosing one of five security levels. By default, the application starts in self-learning mode,

which will automatically configure your security system depending on your responses to various events. This makes your personal guard adjustable to your specific preferences and your particular needs.

Kaspersky® Personal Security Suite

- Kaspersky® Personal Security Suite is a program suite designed for organizing comprehensive protection of personal computers running Windows. The suite prevents malicious and potentially dangerous programs from penetrating through any possible data sources and protects you from unauthorized attempts to access your computer's data, as well as blocking spam. Kaspersky Personal Security Suite has the following features:

- anti-virus protection for data saved on your computer;

- protection for users of Microsoft Outlook and Microsoft Outlook Expressfrom spam;

- protection for your computer from unauthorized access, and also from network hacker attacks from your LAN or the Internet.

Kaspersky® Security for PDA

Kaspersky® Security for PDA provides reliable anti-virus protection for **data saved on various types of Pocket PCs and smartphones.** The program includes an optimal set of anti-virus defense tools:

- **anti-virus scanner** that scans information (saved both on the PDA and smartphones) on user demand;

- **anti-virus monitor** to intercept viruses in files that are either copied from other handhelds or are transferred using HotSync™ technology.

Kaspersky® Security for PDA protects your handheld (PDA) from unauthorized intrusion by encrypting both access to the device and data stored on memory cards.

Kaspersky Anti-Virus® Business Optimal

This package provides a configurable security solution for small- and medium-sized corporate networks.

Kaspersky Anti-Virus® Business Optimal includes full-scale anti-virus protection for:

- Workstations running Windows 98/ME, Windows NT/2000/XP Workstation, and Linux;

- File and application servers running Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Windows 2003 Server, Novell Netware, FreeBSD and OpenBSD, and Linux;
- E-mail clients, namely Microsoft Exchange 5.5/2000/2003, Lotus Notes/Domino, Postfix, Exim, sendmail, and qmail;
- Internet-gateways: CheckPoint Firewall –1; MS ISA Server.

The Kaspersky Anti-Virus® Business Optimal distribution kit includes Kaspersky® Administration Kit, a *unique tool for automated deployment and administration*.

You are free to choose from any of these anti-virus applications, according to the operating systems and applications you use.

Kaspersky® Corporate Suite

This package provides corporate networks of any size and complexity with comprehensive, scalable anti-virus protection. The package components have been developed to protect every tier of a corporate network, even in mixed computer environments. Kaspersky® Corporate Suite supports the majority of operating systems and applications installed across an enterprise. All package components are managed from one console and have a unified user interface. Kaspersky® Corporate Suite delivers a reliable, high-performance protection system that is fully compatible with the specific needs of your network configuration.

Kaspersky® Corporate Suite provides comprehensive anti-virus protection for:

- Workstations running Windows 98/ME, Windows NT/2000/XP, and Linux;
- File and application servers running Windows NT 4.0 Server, Windows 2000, 2003 Server/Advanced Server, Novell Netware, FreeBSD, OpenBSD and Linux;
- E-mail clients, including Microsoft Exchange Server 5.5/2000/2003, Lotus Notes/Domino, Sendmail, Postfix, Exim and Qmail;
- Internet-gateways: CheckPoint Firewall –1; MS ISA Server;
- Hand-held computers (PDAs), running Windows CE and Palm OS, and also smartphones running Windows Mobile 2003 for Smartphone and Microsoft Smartphone 2002.

The Kaspersky® Corporate Suite distribution kit includes Kaspersky® Administration Kit, a *unique tool for automated deployment and administration*.

You are free to choose from any of these anti-virus applications, according to the operating systems and applications you use.

Kaspersky® Anti-Spam

Kaspersky® Anti-Spam is a cutting-edge software suite that is designed to help organizations with small- and medium-sized networks wage war against the onslaught of undesired e-mail (spam). The product combines the revolutionary technology of linguistic analysis with modern methods of e-mail filtration, including RBL lists and formal letter features. Its unique combination of services allows users to identify and wipe out up to 95% of unwanted traffic.

Installed at the entrance to a network, where it monitors incoming e-mail traffic streams for spam, Kaspersky® Anti-Spam acts as a barrier to unsolicited e-mail. The product is compatible with any mail system and can be installed on either an existing mail server or a dedicated one.

Kaspersky® Anti-Spam's high performance is ensured by daily updates to the content filtration database by samples provided by the Company's linguistic laboratory specialists.

Kaspersky SMTP Gateway

Kaspersky® SMTP-Gateway for Linux/Unix is a solution designed for processing e-mail transmitted via SMTP for viruses. The application contains a number of additional tools for filtering e-mail traffic by name and MIME type of attachments and a series of tools that reduces the load on the mail system and prevents hacker attacks. DNS Black List support provides protection from e-mails coming from servers entered in these lists as sources for distributing e-mail.

B.2. Contact Us

If you have any questions, comments, or suggestions, please refer them to one of our distributors or directly to Kaspersky Lab. We will be glad to assist you in any matters related to our product by phone or via email. All of your recommendations and suggestions will be thoroughly reviewed and considered.

Technical support	Please find the technical support information at http://www.kaspersky.com/supportinter.html
General information	WWW: http://www.kaspersky.com http://www.viruslist.com Email: sales@kaspersky.com